On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach

Sahoo, Subham; Chih-Hsien Peng, Jimmy ; Devakumar, Annavaram; Mishra, Sukumar ; Dragicevic, Tomislav

Published in:
I E E E Transactions on Industrial Electronics

DOI (link to publication from Publisher):
10.1109/TIE.2019.2938497

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach

Subham Sahoo, *Member, IEEE*, Jimmy Chih-Hsien Peng, *Member, IEEE*, Annavaram Devakumar, Sukumar Mishra, *Senior Member, IEEE* and Tomislav Dragičević, *Senior Member, IEEE*

***Abstract*—Though recent advancements in DC microgrids are largely based on distributed control strategies to enhance reliability and scalability, the absence of a centralized controller to check the global information makes these schemes highly susceptible to cyber attacks. Since false data injection attacks (FDIAs) are considered as a prominent attack methodology in DC microgrids, prior emphasis is usually laid on compromised sensors and controllers only related to DC voltages. Hence, this paper firstly segregates the FDIAs on the output currents into *destablization* and *deception* attacks, based on the modeling of attack elements with respect to the consensus theory. Secondly, a discordant element based detection approach is designed to detect the attacked nodes accurately, using an extended analysis of the cooperative control network. A risk assessment framework for DC microgrids against cyber attacks is provided alongside all the case studies. An evaluation theory is also presented to assist the proposed detection scheme to differentiate between cyber attacks and faults. Further, the proposed detection approach is theoretically verified and validated using simulation and experimental conditions.**

***Index Terms*—DC microgrid, cyber attacks, distributed control, cyber-physical systems.**

I. Introduction

THE rapid development of DC microgrids can be ascribed to their high flexibility in integrating renewable energy sources, storage devices and modern electronic loads, in both grid-connected and autonomous modes of operation [1]. Compared to a centralized framework that is vulnerable to a single point-of-failure, a distributed control structure is considered as a scalable and efficient control architecture to manage a network [2]. Moreover, distributed communication ensures robust performance under cyber imperfections such as communication delays, link failures and data packet losses [3]. The main philosophy behind distributed control in DC microgrids is to achieve average voltage regulation [4] and proportionate load current sharing [5] between the participating agents. These operations are conventionally carried out with the assumption of a reliable cyber network reporting *true* measurements [6]. However, any physical violation or erroneous measurement in the microgrid degrade the system operation or lead to unstable performance [7]. Such events can occur in the presence of cyber attacks, which can be introduced by illegitimate data intrusion into the cyber-physical components such as sensors and communication links.

Cyber attacks are a growing concern for modern power systems, which therefore strives for security enhancements. Such attacks can take place using various intrusion techniques, which can be divided into several categories such as false data injection attacks (FDIAs) [8], denial of service (DoS) [9] and replay attacks [10]. They are all capable of disrupting the network stability and control structures. This paper focuses on investigation of FDIAs, as the most prominent cyber attack example. To alleviate the burden of singularity in centralized systems, distributed control can be an alternative approach for improved security. However, distributed schemes are more vulnerable to cyber attacks due to the propagation of attack element into the neighbors. Such attacks can take place in micorgrids remotely, using compromised data, communication protocols and cyber channels.

Cyber attacks can also be *coordinated*, where the attacker attains sufficient knowledge about the system involving control and network architecture to create attack vectors, which can easily bypass the well-defined bad-data detection tests [11]. Such data intrusion method can be categorized as generalized FDIA, which is also commonly termed as a *stealth* attack [12]. In the context of DC microgrids, a stealth attack ensures a zero neighborhood tracking error for each agent as discussed in [13]. The attacker can use this *discreet* behavior to attack microgrids by penetrating into the control system deceitfully, and cause instability later in unforeseeable ways. Since the control objectives in DC microgrids can be maneuvered artificially to cause instability, the risk assessment against such attacks requires significant attention.

Considerable research to quantify the impact on DC microgrid using FDIAs and DoS attacks is done using candidate invariants in [14] and hyperproperties in [15]. Referring to [16], active defense watermarking techniques, which are used to detect such intrusions using a set of feedback signals, can generate unlikely output under attacks. However, the design of the abovementioned approaches are quite complex as it requires accurate model checking tools. It gives rise to increased computational burden and complications. Moreover, artificial intelligence based data driven tools can exploit the unbiased state variables of any plant to determine the attacked node.

This work was supported in part by the National Research Foundation, Singapore under Grant NRF2018-SR2001-018.

S Sahoo and T Dragičević are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: sssa@et.aau.dk and tdr@et.aau.dk)

J Peng is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 119007 (e-mail: jpeng@nus.edu.sg)

A Devakumar and S Mishra are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi-110016 (e-mail:devakumarannavaram@gmail.com and sukumar@ee.iitd.ac.in)

Nevertheless, the conundrum behind the presence of attack elements in any dataset will always remain a concern. For such simplistic models, Sahoo *et. al.* in [13] have proposed a stealth attack detection strategy for false data intrusion into voltage sensors. Intuitively, the basic philosophy behind power flow control in DC microgrids is by controlling the voltages, which draws primary attention to the associated voltage counterparts only for cyber attacks.

Considering these issues, this paper firstly studies two variants of false data injection into current sensor(s), namely destabilization and deception attacks. Secondly, a fully distributed discord element based detection strategy is proposed to identify the attacked agent, by extending basic principles of consensus theory. As a result, the effective cost and resources required to implement this scheme on an already established prototype is minimal. A theoretical framework for both variants of attacks is provided using the converter equations to validate the detection theory. Risk assessment of the attacks and their impact on microgrids have been analyzed to understand the critical liabilities at risk. Differentiation between faults and cyber attacks is also carried out using an evaluation theory, which assists the proposed detection scheme to avoid false tripping of relays. To test the robustness of the proposed detection scheme, it has been evaluated under multiple scenarios including communication delay, plug in-and-out of converter(s) using attack models of varying severity. The performance has been validated under simulation and experimental conditions to conclude that the proposed detection scheme can reliably detect the presence of attacks and sunbsequently activate the appropriate defense mechanisms. To the best of authors' knowledge, the proposed detection strategy has never been proposed in detecting FDI attacks in DC microgrids.

The rest of the paper is organized as follows. Section II depicts a brief overview of the cyber-physical architecture of DC microgrids alongwith a basic overhaul of distributed secondary control objectives and equations. A comprehensive risk assessment framework alongwith definition and characterization of FDI attacks is provided in Section III. Section IV depicts the proposed detection scheme with theoretical analysis. Simulations along with experimental validation are presented in Section V and VI, respectively. Finally, Section VII provides the concluding remarks and future scope of this work.

II. Conventional Distributed Control Strategy in DC Microgrids

An exemplary autonomous DC microgrid considered in this work is shown in Fig. 1. N DC sources connected via DC/DC converters of equal power rating are interconnected to each other via tie-lines forming the physical layer of the microgrid. DC/DC converters are operated in voltage controlled mode. Droop control philosophy ensures equal current sharing by imposing voltage offset error. To compensate for this offset, secondary controllers are deployed [17]. In the cyber layer, an undirected graph is considered, where vertices denote the points of connections of physical sources (DC/DC converters).

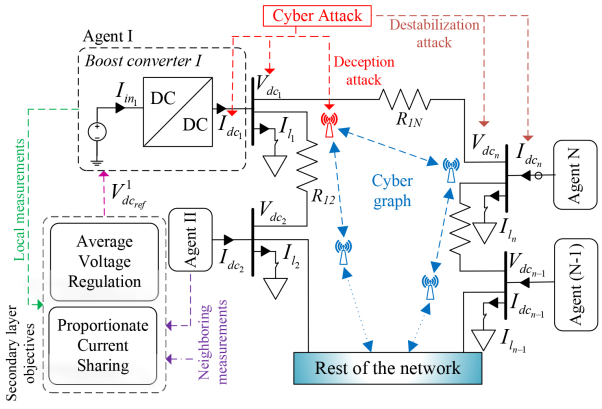

Fig. 1. Generic cyber-physical model of DC microgrid with N agents: Blue arrows represent the cyber layer and black lines represent the physical circuit. Red and brown lines represent deception and destabilization attacks, respectively. The local and neighboring measurements are indicated by green and violet lines, respectively.

Each vertex sends and receives $\psi_j = \{\bar{V}_{dc_j}, I^{pu}_{dc_j}\}$ from its neighboring vertices to achieve average voltage regulation and proportionate current sharing, where $\bar{V}_{dc_j}$ and $I^{pu}_{dc_j}$ denote the average voltage estimate and per unit output current of the neighboring agents. Each agent is represented via a node and a communication digraph via edges using an adjacency matrix $\mathbf{A} = [a_{ij}] \epsilon R^{N\times N}$. The communication weights are given by:

$$a_{ij} = \begin{cases} > 0, & \text{if } (x_i, x_j) \epsilon \mathbf{E} \\ 0, & \text{else} \end{cases}$$

where $\mathbf{E}$ is an edge connecting two nodes, with x_i and x_j being the local and neighboring node respectively. Using the cyber graph, the local input can be written as:

$$u_i = \sum_{i \in M_i} a_{ij}(\psi_j - \psi_i) \tag{1}$$

where $u_i = \{u^V_i, u^I_i\}$ corresponding to the elements in ψ and M_i denote the set of neighbors of i^{th} agent. Mathematically, the incoming information matrix can be denoted by $\mathbf{Z}_{in} = \sum_{i\ \epsilon\ N} a_{ij}$. Hence, if both matrices match each other, the Laplacian matrix $\mathbf{L}$ is *balanced*, where $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$ and its elements are given by:

$$l_{ij} = \begin{cases} \deg(n_i) & , i = j \\ -1 & , i \neq j \\ 0 & , \text{otherwise} \end{cases} \tag{2}$$

where $\deg(n_i)$ is the degree of i^{th} agent.

Remark I: *As per the synchronization law [19], all the agents participating in distributed control will achieve consensus using* $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ *for a well-spanned matrix* L *such that* $\lim_{t\to\infty} x_i(t) = c,\ \forall i\ \epsilon\ N$, *where* c *is the steady-state reference and* N *is the number of agents.*

To establish these objectives for DC/DC converters operating to maintain output voltage, two voltage correction terms

for i^{th} agent are calculated using:

$$\Delta V_{1_i} = H_1(s)\underbrace{(V_{dc_{ref}} - u_i^V)}_{e_i^V} \tag{3}$$

$$\Delta V_{2_i} = H_2(s)\underbrace{(I_{dc_{ref}} - u_i^I)}_{e_i^I} \tag{4}$$

where $H_1(s)(= K_P^{H_1} + \frac{K_I^{H_1}}{s})$, $H_2(s)(= K_P^{H_2} + \frac{K_I^{H_2}}{s})$ are PI controllers and $V_{dc_{ref}}$ and $I_{dc_{ref}}$ are the global reference voltage and current quantities for all the agents, respectively. It should be noted that $I_{dc_{ref}}$ = 0 for proportionate current sharing between the agents. The correction terms obtained in (3)-(4) are finally added to the global reference voltage $V_{dc_{ref}}$ setpoint to achieve local voltage references for i^{th} agent using:

$$V_{dc_{ref}}^i = V_{dc_{ref}} + \Delta V_{1_i} + \Delta V_{2_i}. \tag{5}$$

Using (5) as the local voltage reference for i^{th} agent, the secondary objectives highlighted in Fig. 1 is achieved.

III. Definition and Risk Assessment of FDI Attacks in DC Microgrids

The *intent* of cyber attacks could be either aimed at immediate destabilization of the microgrid or to deceive the system operator by penetrating the control system in a discreet manner. This discretion can be tactfully used by the attacker for detailed analysis of the network behavior, parameters and then utilize the available data to plan and execute a coordinated FDI attack, which can cause immediate shutdown of the microgrid.

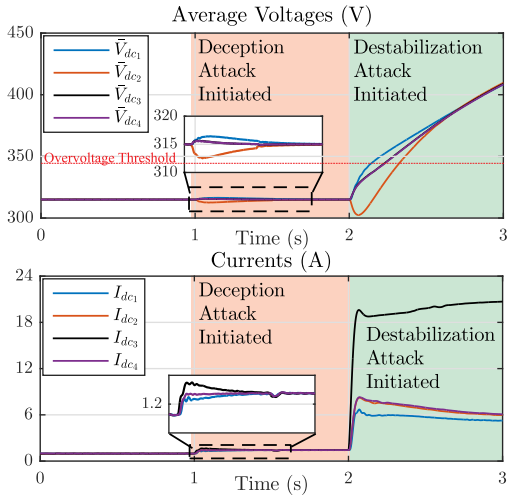

Fig. 2. Case study–A symmetric attack element causes deception at t=1 s adhering to (6), however an asymmetric attack element at t=2 s destabilizes the operation.

Using the distributed consensus algorithm for a well connected cyber graph in a DC microgrid, the system objectives for DC microgrids using (1)-(5) shall converge to:

$$\lim_{t\to\infty} \phi_i(t) = V_{dc_{ref}}, \ \lim_{t\to\infty} u_i^I(t) = 0 \ \ \forall i \ \epsilon \ N \tag{6}$$

where $\phi_i(t) = V_{dc_i}(t) + \int_{j \ \epsilon \ N_i} u_i^V(t)$ with V_{dc_i} denoting the output voltage of i^{th} agent. However, under attacks, the system resorts into a different operating condition, given by:

$$\lim_{t\to\infty} \phi_i(t) = V_{dc_{ref}}^a, \ \lim_{t\to\infty} u_i^I(t) \neq 0 \ \ \forall i \ \epsilon \ N \tag{7}$$

where $V_{dc_{ref}}^a \neq V_{dc_{ref}}$.

Definition 1: Any FDI attack which results in the control inputs converging as per (7) during the operation of DC microgrids can be defined as ***destabilization attack***.
In particular, network stability is compromised if certain voltage bounds in the buses are exceeded, because over- and under-voltage relays may trip. The attack can be formulated in such a manner that the voltages of each agent go outside the allowable operational limit.

Assuming a pre-condition that the system always operates at a certain global reference voltage, which is known to each agent, (7) should be a sufficient criteria to justify that the system is attacked by an external entity. However, some attacks can be conducted with more sophistication such that the attack occurs, yet the system satisfies (6).

Definition 2: Any FDI attack which results in the control inputs converging as per (6) during the operation of DC microgrids can be defined as ***deception attack***.
Basically, such attacks allow the attacker to penetrate into the control system without affecting control objectives. Such sophisticated attacks can have adverse effect in the long run as the attacker has access to multiple nodes and can create unintentional generation outage, which may eventually lead to loss of functionality. Under these circumstances, detection of the attacked agent(s) under both the classes of attacks in a distributed network is an important aspect to prevent the system from further instability.

Since stealth attacks on voltage sensors, which creates misbehavior with the voltage observer in DC microgrids, has already been studied in [13], this paper focuses on detection of destabilization and deception attacks on current sensors. Using this information, the attack in i^{th} agent can be modeled as follows:

$$\text{Sensor attack:} \quad x_i^f = x_i + \kappa x_i^a \tag{8}$$

$$\text{Cyber link attack:} \quad x_{ij}^f = x_{ij} + \kappa x_i^a \tag{9}$$

where κ = 1 denotes the presence of an attack element x_i^a in the measurement x_i in i^{th} agent, or 0 otherwise. It is worth notifying that the sensor and cyber link attacks can be conducted separately by hijacking the controller and communication server, respectively [13].

A case study is done in Fig. 2 on a DC microgrid with N=4 agents to show the impact of deception and destabilization attacks on current sensors. When an attack element of I_{dc}^a = {0, 0, 5, 0} A is introduced into the sensor and communication link at t = 1 s, the output currents increase equally as if there is a change in load. Moreover, the average voltage is regulated back to $V_{dc_{ref}}$ = 315 V. As per Definition 2, all the necessary conditions are met, which certifies it as a deception attack. However at t = 2 s, another attack element is introduced only into the sensors with I_{dc}^a = {0, 0, 20, 0} A. It can be seen that the output currents increase invariably with the

voltages ramping up. As the voltages reach close to overvoltage threshold (highlighted in Fig. 2), it could potentially lead to the shutdown of the system. It is worth notifying that the case study in Fig. 2 is done without considering any relays or protection devices to provide a clear picture of the consequences caused by destabilization attacks. Hence the attacker deceitfully infiltrates into the control system of agent III at t = 1 s and causes a destabilization attack later, as per Definition 1.

Remark II: *From the case study in Fig. 2, it can be determined that the attack element has to be symmetric in case of a deception attack, such that the false data is injected locally(sensors) and the neighbors(transmitted via communication) to satisfy:*

$$\dot{\mathbf{I}}^a_{dc} = \mathbf{L}\mathbf{I}^a_{dc}. \tag{10}$$

If the above condition is not true, it will lead to a destabilization attack.

To extend the analysis of the modeled attacks in Remark II, a set of eigenvalues to represent the system and attack dynamics, Ξ_S and Ξ_A respectively, can be defined as:

$$\Xi_S = \{\lambda^1_S, \lambda^2_S, ..., \lambda^N_S\} \tag{11}$$

$$\Xi_A = \{\lambda^1_A, \lambda^2_A, ..., \lambda^N_A\} \tag{12}$$

where λ denote the respective eigenvalues. A detailed state-space modeling of cooperative DC microgrids can be referred from [18].

Remark III: *Considering the attack models in (8)-(9) with $\mathbf{I}^a_{dc}$ defined in (10), injecting an attack signal into any node,*

1) *destabilizes the system, if $\Xi_S \cap \Xi_A \neq 0$, $u^I_i \neq 0$. These attack models are categorized as destabilization attacks.*
2) *leads to a feasible and stable solution, if $\Xi_S \cap \Xi_A = 0$, $u^I_i = 0$. These attack models are categorized as deception attacks.*

As outlined in the abovementioned case study, unexpected risks can be introduced in cooperative DC microgrids using both variants of FDI attacks. Hence, a risk assessment framework is provided for DC microgrids to quantify the risk imposed to critical infrastructures. The risk assessment (RA) index can be given by:

$$\textbf{\textit{RA}} = \textbf{\textit{IA}} \text{ x } \textbf{\textit{MO}} \tag{13}$$

where ***IA*** denotes the intrusion access index, which indicates the number of compromised sensors in an agent and ***MO*** denotes the microgrid outage index, which suggests the physical outcome to the microgrid infrastructure due to the FDI attack. The conditional visualization of the abovementioned indices is provided in Table I.

TABLE I
CONDITIONAL VISUALIZATION OF RISK ASSESSMENT FOR FDI ATTACKS IN DC MICROGRIDS

Intrusion Access Index		Microgrid Outage Index	
Single Sensor or Cyber Link	1	Line Outage	1
Single Sensor & Cyber Link	2	Converter Outage	2
Multiple Sensors & Cyber Links	3	Shutdown	3

Using (13), it can be deduced that the risk concerns are at the lowest in DC microgrids for ***RA*** = 1 and increases until 9. Moreover, since this study is based on determining the maximum casualty prior to any FDI attack, the maximum value of ***MO*** index shall always be considered in the case of cascaded events. For the case study in Fig. 2, the ***RA*** index will amount to 4 (i.e, 2x2) since the converter in agent III has to be plugged out to restore the operation. Converter outage increase the loading on the remaining converters, which may run into overloading during highly loaded conditions. It is worth noting that the indices have been ranked considering the loss of functionality prior to each event. Based on different attack models, it is intuitive that the access indices have predefined boundaries of causing cyber-physical outcomes in DC microgrids. For example, a single sensor attack (***IA*** = 1) in any agent may dismantle the control loop as per Remark II, leading to an overvoltage condition. As a result, the overvoltage relays cause plugging out of the converter to ensure stability of the rest of the system. Moreover, this situation may turn fatal if the abovementioned attack is carried out in a bus with high loading, which exceeds the overcurrent continuous flow limits of a line, causing line outage. Consequently, the ***MO*** index for the abovementioned scenario is limited between 1 to 2. Finally, the ***MO*** outcomes can be quantified with factors such as the magnitude of attack vectors, symmetricity of attack elements' distribution in the microgrid and the cyber topology. A similar analogy can be followed for the rest of the ***IA*** indices.

Hence, the consequences of an attack can be identified in conjunction with the proposed risk assessment index to identify the most important risks to be managed. Moreover, it should be noted that the line and converter outages are caused by relays, which are set to operate on certain overvoltage and overcurrent threshold values. Using this framework, the severity of both variants of FDI attacks can be quantified to formalize the detection and defense measures accordingly.

IV. PROPOSED DISCORDANT ELEMENT BASED DETECTION STRATEGY

This section involves discussion of the proposed discordant element (DE) based detection approach for both categories of FDI attacks in a cooperative DC microgrids. The basic challenge lies in determining the attacked agent in cooperative network, which becomes more appealing as the transmitted false data in any given agent also propagates to its neighbors.

1) Destabilization Attacks: Considering a constant signal attack on current sensor in i^{th} agent using Remark II & III, it can be written as

$$\mathbf{L}\mathbf{I}^a_{dc} \neq 0 \tag{14}$$

Under such case, the output currents from all the agents will not be shared equally. Consequently, the solution to cooperative synchronization error for output currents using Remark I under such attacks can be written as:

$$\mathbf{e}^I(t) = \mathrm{e}^{-h_v \mathbf{L} t}\mathbf{e}^I(0) + \int_0^t \mathrm{e}^{-h_v \mathbf{L}(t-\tau)}\mathbf{k} d\tau \tag{15}$$

where $\mathbf{k} = \eta \mathbf{L}\mathbf{e}^{I^a}$, where η is a diagonal matrix which indicates the presence of attack in the current sensor using

a non-zero value. For positive-definite values of $\mathbf{L}$ and h_V, the first term in (15) goes to zero. Using $\mathrm{e}^{At} = \sum_{i=1}^{\infty}(At)^i$, the final steady state value of (15) is given by

$$\mathbf{e}^I(t) \rightarrow \sum_{i=1}^{\infty} \int_0^t (-h_V(\mathbf{L}(t-\tau))^i d\tau \tag{16}$$

Hence, for non-zero elements in the Laplacian graph, $l_{ij} \neq 0$, the synchronization error in (16) converges to a non-zero value. As a result, the synchronization error leads to a ramped up/down quantity for ΔV_{2_i} corresponding to the output of PI controller in (3). Using this condition as a sufficient criteria, it can be alternatively termed as output currents from each bus are in *discord* with each other for a non-zero synchronization error. Hence, the operational dynamics of secondary sublayer I will not obey consensus theory as per [13].

2) Deception Attacks: However in case of deception attacks, the cooperative synchronization law holds true as per Remark II & III for *symmetric* attack vector in current sensors and communication links. Hence, ϕ obeying Remark I, can be written in vector form as:

$$\dot{\bar{\mathbf{V}}}_{dc} + \mathbf{L}\bar{\mathbf{V}}_{dc} = \dot{\mathbf{V}}_{dc} = 0 \tag{17}$$

Moreover, the voltage dynamics at each bus in vector form can be written as:

$$\dot{\mathbf{V}}_{dc} = \mathbf{C}^{-1}(\mathbf{D}_k\mathbf{I}_{in} - \mathbf{I}^f_{dc}) \tag{18}$$

where $\mathbf{D}_k = 1 - \mathbf{D}$. Further, $\mathbf{I}_{in}$, $\mathbf{D}$, $\mathbf{C}$ and $\mathbf{I}^f_{dc}$ denote the diagonal matrices of the input current I_{in_i}, duty ratio D_i, DC link capacitance C_i and the attacked output current measurement I_{dc_i} respectively for N agents. Since the average voltage estimates aren't compromised, they adhere to the global reference.

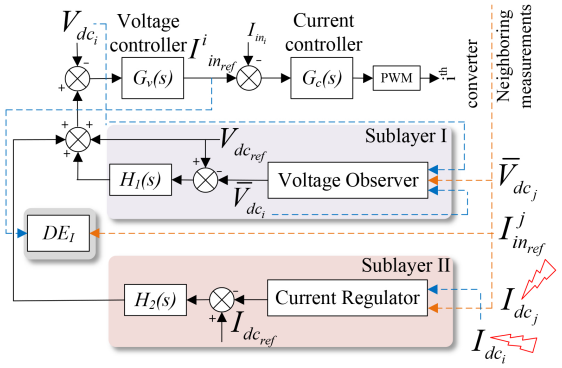

Fig. 3. Proposed discordant element based detection controller using local and neighboring measurements for i^{th} agent in DC microgrids– DE_I to detect anomalies in the current counterparts.

Considering the error dynamics into the voltage controller under steady-state conditions, we get:

$$\mathbf{L}^T\Delta\mathbf{V}_1 + \mathbf{L}^T\mathbf{H}_2\mathbf{e}^{Ia} + \mathbf{V}_{dc_{ref}} = \mathbf{L}^T\mathbf{V}_{dc} \tag{19}$$

where $\mathbf{e}^{Ia}$ denotes a diagonal matrix of the error quantity in (1) with attacked current signals.

Remark IV: *Since the system objectives in (6) are met for a deception attack, $\mathbf{L}^T\Delta\mathbf{V}_1 = 0$ holds true [13].*

Using Remark IV and differentiating (19), we get:

$$\mathbf{L}^T\mathbf{K}_P^{H_2}\dot{\mathbf{e}}^{Ia} + \mathbf{L}^T\mathbf{K}_I^{H_2}\mathbf{e}^{Ia} - \mathbf{L}^T\dot{\mathbf{V}}_{dc} = 0. \tag{20}$$

In steady state, $\mathbf{e}^{Ia} = 0$. Further using Remark III, $\mathbf{L}^T\mathbf{C}^{-1}\mathbf{I}^a_{dc} = 0$. Using these equalities after substituting (17) in (18), we get:

$$\mathbf{L}^T\mathbf{K}_P^{H_2}\dot{\mathbf{e}}^{Ia} - \mathbf{L}^T\mathbf{C}^{-1}\mathbf{D}_k\mathbf{I}_{in} = 0. \tag{21}$$

Remark V: *Due to the injected attack signal, the first term of (21) will be asymmetric, as explained in (16). For (21) to hold true, this property will be reflected in the second term of (21), which becomes the basis of detection for false data injection attacks in cooperative DC microgrids.*

Using Remark V, it is intuitional that $\mathbf{L}^T\mathbf{I}_{in}$ will always converge to zero under no attacks for normalized duty ratios D_i across the microgrid. Hence, it has been proved that the normalized input current reference quantities also achieve consensus among themselves for a constant global reference voltage at the output of their respective DC/DC converters in DC microgrids.

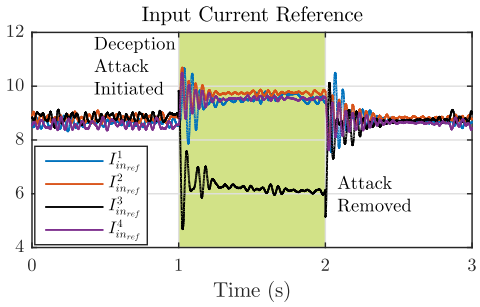

Fig. 4. Performance evaluation of discordant theory in the input current references when subjected to deception attack on Agent III in DC microgrids- $I^3_{in_{ref}}$ does not obey cooperative synchronization under the attack.

As shown in Fig. 3, the input current I^i_{in} is controlled using a reference current value obtained from the outer voltage controlled loop. Hence for an attack in secondary sublayer II output prior to a deception attack, it causes the outer voltage loop to operate differently for each agent. Since a load change in i^{th} agent introduces a voltage transient dip, this forms a positive voltage error for the non-attacked agents. However for the attacked agent, this error will be negative since the secondary sublayer II output maloperates as a result of the compromised current information. It has been clearly shown in Fig. 4 that the compromised agent's current reference goes discordant with the remaining agents to authorize the discordant element based detection theory.

Definition 3: A state variable that does not obey consensus theory in the presence of cyber attack is said to be in a ***discordant*** *state.*

To account for this discord effect, a discordant element for current counterparts, DE^i_I is proposed using the local and neighboring measurements to detect likely attacks on the output current sensors and cyber links of i^{th} agent using:

$$DE^i_I = l_i[\sum_{j\epsilon M_i} I^j_{in_{ref}} - I^i_{in_{ref}}][\sum_{j\epsilon M_i} I^j_{in_{ref}} + I^i_{in_{ref}}] \tag{22}$$

where $I^i_{in_{ref}}$ is the reference input current obtained from the outer voltage control loop in i^{th} agent. Moreover, l_i is a positive quantity, which is used to increase/decrease the value of DE^i_I. Hence by a similar definition for DE^i_I, any positive value in (22) will reflect an attack in the current counterparts of i^{th} agent. Another fortcoming point is that any data intrusion in the input current sensors would not affect the system response under any circumstances. This resiliency can be attributed to the fact that it is a part of the nested control loop for DC/DC converter shown in Fig. 3. Concluding the above remarks, any likely attack on the current counterparts of i^{th} agent in DC microgrid can be determined by monitoring positive values for DE^i_I, which can be alternatively written as:

$$DE^i_I = \begin{cases} 0, \textbf{if } \kappa = 0 \\ > 0, \textbf{else} \end{cases} \tag{23}$$

Hence, (23) provides an unified and fully distributed discordant element based attack detection scheme in DC microgrids for the abovementioned variants of FDI attacks.

V. Simulation Results

The proposed detection theory is tested on cyber-physical DC microgrids with N= 4 agents, as shown in Fig. 1. Each agent of equal power capacities comprising of a DC source and DC/DC boost converter, operate to maintain output voltage for a global reference $V_{dc_{ref}}$ = 315 V at their respective buses. The robustness of the proposed DE based detection theory has been tested for deception attacks on single and multiple agents in DC microgrids (***IA*** = [2, 3]), which goes undetected by distributed voltage observer. Furthermore, it is also tested for destabilization attacks (***IA*** = 1) on accurate identification of the attacked counterparts in any agent. It should be noted that each event in the abovementioned detection scenarios are separated by a certain time-gap to provide clear understanding. Moreover, the attack vector I^a_{dc} consist of attack elements for each agent in the order of $\{I^a_{dc_1}, I^a_{dc_2}..., I^a_{dc_N}\}$. The simulation plant and control parameters are provided in Appendix.

In the first case study in Fig. 5, a destabilization attack is injected using the attack elements I^a_{dc} = {0, 2.4, 0, 3.2} A into the current sensors respectively in multiple agents in DC microgrids, i.e, agent II and IV at t = 2 s. Since the sensors are attacked, it falls under the category ***IA*** = 1. As soon as the attack is initiated, the current sharing among agents grow disproportionate, which leads to a non-zero error into the secondary sublayer II. As a result, ΔV_{2_i} of each agent starts ramping, thereby dissembling the final references in each agent, which impairs the global voltage regulation as shown in Fig. 5. Under such scenarios, the microgrid may run into a state ***MO*** > 2, leading to loss of functionality. Hence, the ***RA*** index using such attacks is limited to 2 as per (13). As per the proposed detection theory in (23), both $\{DE^2_I, DE^4_I\}$ indicate a positive value, as shown in Fig. 5, for the attacked agents II and IV. Upon detection, the attack is removed from the affected agents at t = 3 s, which brings back the system into following the control objectives in (6).

Next, a deception attack is injected in Fig. 6 using the attack elements I^a_{dc} = {0, 1.6, 1.8, 0} A into the current sensors and cyber link respectively into agents II and III at t = 1 s. As per Table I, it can be categorized under ***IA*** = 2. When the attack is initiated, it can be seen in Fig. 6 that the voltages at each bus are still distributed around the global reference of $V_{dc_{ref}}$ = 315 V. Moreover, as a result of the false data injection into the current sensors and cyber link, a visual imprint of load change is created without any actual physical disturbance. This behavior deceives the system operator, thereby adhering to the control objectives, otherwise. Such attacks can be critical as this action can be deceitfully used by the attacker to cause destabilization in DC microgrids later. Identifying such conditions as a severe risk to infiltrate large attack vectors later, it can cause critical damage to the system by shutting down both converters (***MO*** > 2). Hence, the ***RA*** index lies in the range of [4, 6]. As per the proposed attack detection theory for deception attacks, DE^2_I and DE^3_I goes positive at t = 2 s to indicate the presence of false data elements for the current counterparts in agent II and III. When the attack is removed, the proportionate current sharing and voltage regulation inputs operate normally with *unbiased* measurements. More details on mitigating techniques for such attacks can be referred from [15].

To demonstrate the resiliency of attacks for false data injection into the input current sensor, another attack (highlighted as Attack II) is introduced at t = 3 s in Fig. 6, which does not create further exploitation in the system since the reference signal for input current $I_{in_{ref}}$ is generated as a nested loop control output. It can not be exploited by data intrusion in a closed loop voltage regulated control system.

To differentiate between faults and cyber attacks, a case study is presented in Fig. 7 for a short time-scale ($\approx$ 100 ms) illustrating the response of a DC/DC converter in case of FDI attacks and faults. It should be noted that the origin in Fig. 7(b) is ($V_{dc_{ref}}$, I_{dc}), where I_{dc} will vary between the minimum and maximum current limit based on the loading level. A *boundary of operation* region is defined in Fig. 7(a), which varies within {X $\in$ [V_{in}, 1.3$V_{dc_{ref}}$], Y $\in$ [I_{min}, I_{max}]}. It can be observed that positive and negative destabilization attacks cause the trajectories to move into Quadrant I and III respectively. Further, deception attacks with a feasible solution operate either in Quadrant II/IV corresponding to an increase in load in the same/different bus. This behavior can be attributed to the response of the distributed secondary controller in (3)-(5). However, in case of DC line-to-line faults, the response of the primary control layer results in a large increase in the output current alongwith a decrease in output voltage. This behavior can be clearly seen in Fig. 7(a) where the fault trajectory goes out of the boundary of operation in less than 100 ms. Since the timescale separation between the secondary and primary layers is considerably large, this evaluation theory (within a certain time frame $\approx$ 100 ms) can be used locally as a substantial indicator to assist the proposed detection scheme in differentiating between faults and cyber attacks.

Next, the response of output currents following the considered attacks is discussed. Referring to Fig. 6, it can be seen that the output currents rise to a new value when a constant valued deception attack is initiated at t = 1 s. Using Remark IV, it has

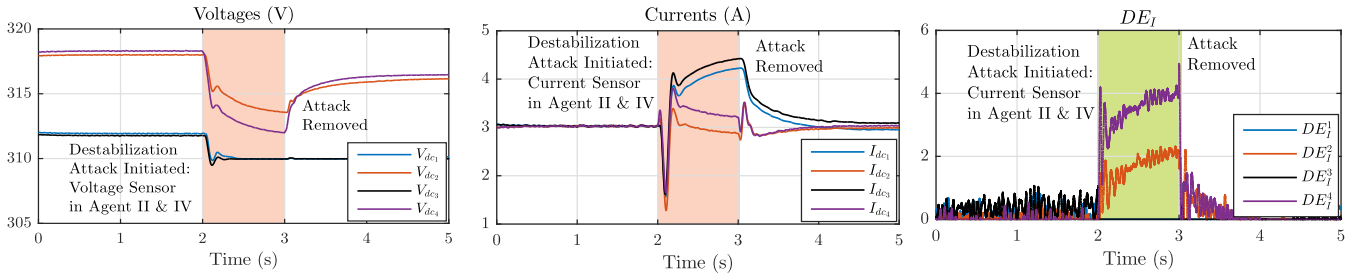

Fig. 5. Performance of the proposed detection strategy under destabilization attack on current sensors in agent II and IV– DE_I for agents II and IV indicate positive values beyond their bounds suggesting that the current sensors of agent II and IV are injected with false data.

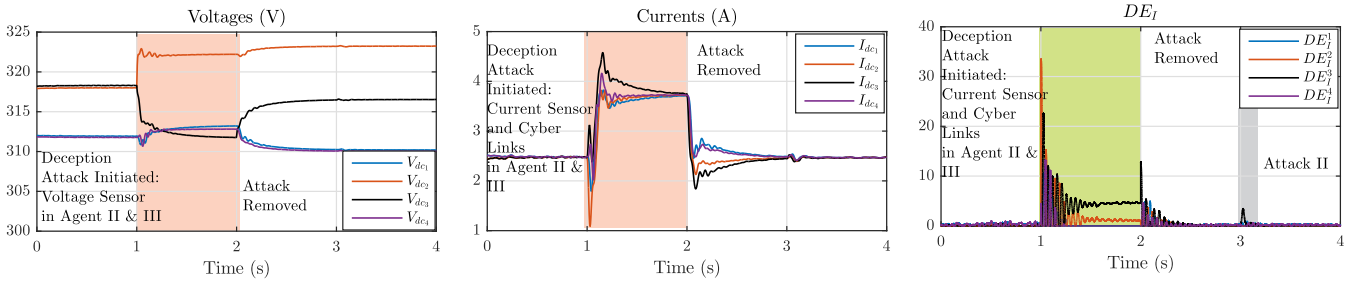

Fig. 6. Performance of the proposed detection strategy under deception attack on current sensors and cyber links in agent II and III– DE_I for agents II and III becomes positive as soon as the attack is initiated. Attack II carried out in the input current sensor of agent II can not be further exploited as $I_{in_{ref}}$ is a control output in the closed loop voltage regulation.

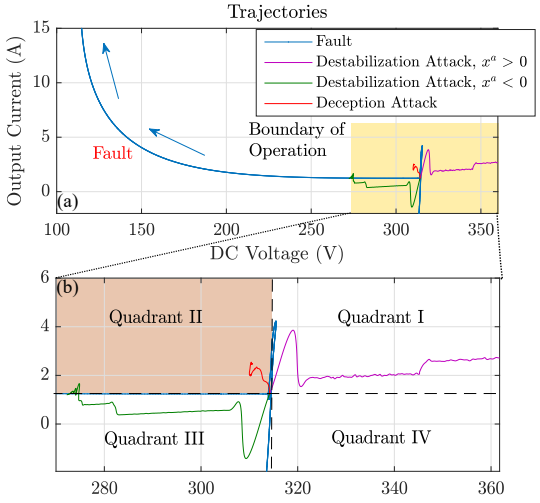

Fig. 7. (a) Response of DC/DC converter in a distributed control based DC microgrid to attacks and faults for 100 ms– Quadrant II shows the faulted area outside the boundary of operation, (b) Zoomed picture of the boundary of operation.

been proved in [13] that $\Delta \mathbf{V}_1 = 0$ when the generation-demand balance is maintained. With this hypothesis, when the attack is initiated, it can be seen in Fig. 6 that it causes a rise in ΔV_2 for (N-1) agents (excluding the attacked agent) in the secondary sublayer in (4). Consequently, the voltage reference for each agent in (5) evolve to obey Remark IV. Since the loads in Fig. 6 are voltage-dependent, the active power demand increases. There is also a rise in the difference of the output voltage as each agent compensates for tie-line losses. As a result, the output currents rise to a feasible solution following a deception

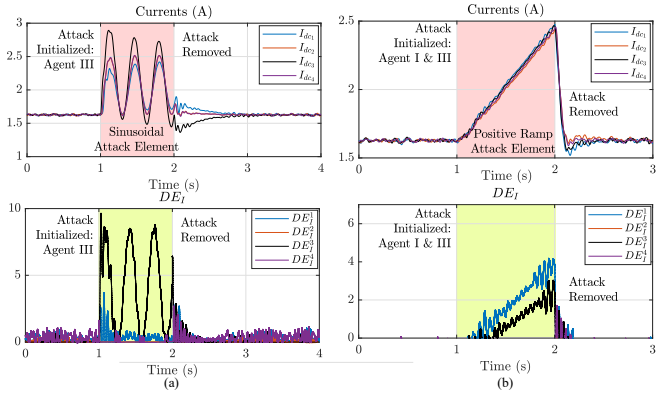

Fig. 8. Performance of the proposed detection strategy using two different attack models: (a) A deception attack (***IA*** = 2) modeled as $I^a_{dc_3} = (1 + 0.8\sin\ 0.4\pi t)$ A on agent III at t = 1 s, (b) Deception attack (***IA*** = 3) modeled as $\{I^a_{dc_1}, I^a_{dc_3}\} = 1.5$t A on agent I and III at t = 1 s.

attack to compensate for the increased demand and line losses. This behavior is a critical issue in autonomous DC systems with batteries as the prime sources.

To test the robustness of the proposed detection strategy, a deception attack $I^a_{dc_3} = (1 + 0.8\sin\ 0.4\pi t)$ A is injected into agent III at t = 1 s in Fig. 8(a). It can be seen that the sinusoidal trace is in the positive DE_I region for agent III. Further, two deception attacks $\{I^a_{dc_1}, I^a_{dc_3}\} = 1.5$t A are injected into agents I and III simultaneously at t = 1 s in Fig. 8(b). As per the proposed detection criteria, ramp traces are observed for both DE^1_I and DE^3_I. This establishes robustness of the proposed scheme in detecting false data attacks in the realm of DC microgrids.

The performance of the proposed scheme to detect cyber

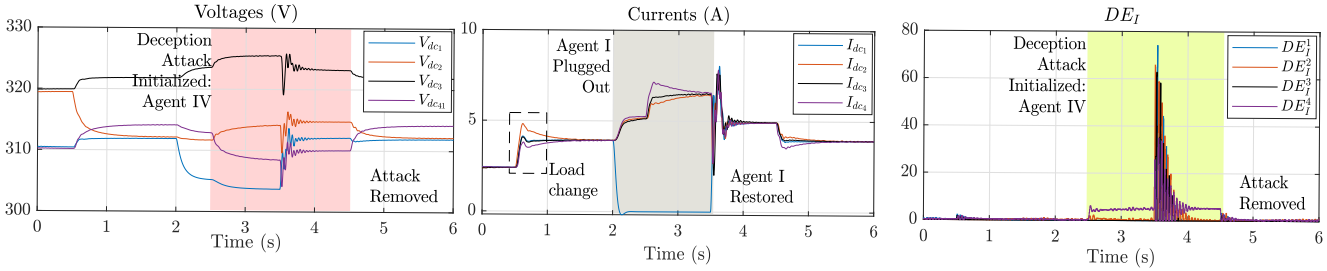

Fig. 9. Performance of the proposed detection strategy under deception attack (***IA*** = 2) in agent IV– Positive DE_I for agent IV indicates the presence of attack even when agent I is plugged in and out at t = 2 and 3.5 respectively.

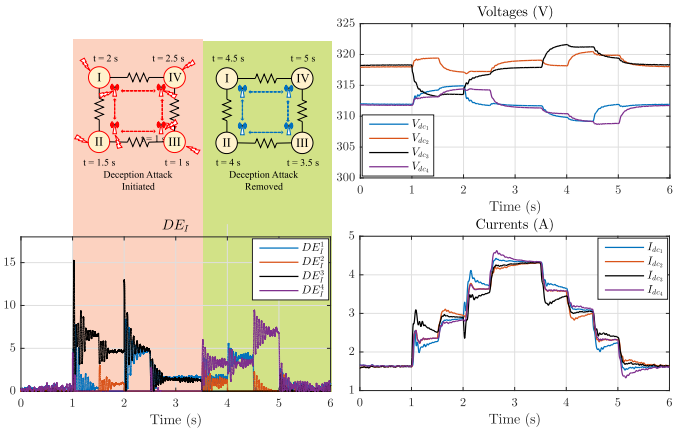

Fig. 10. Performance of the proposed detection strategy under deception attack initiated in a sequence on current sensors & cyber links in all the agents after a gap of 0.5 s starting from t=1 s– During t= 2.5-3.5 s, only DE_I^1 and DE_I^3 are in the detection zone, thereby suggesting the critical boundary of the proposed detection strategy under highest access index level (***IA*** = 3).

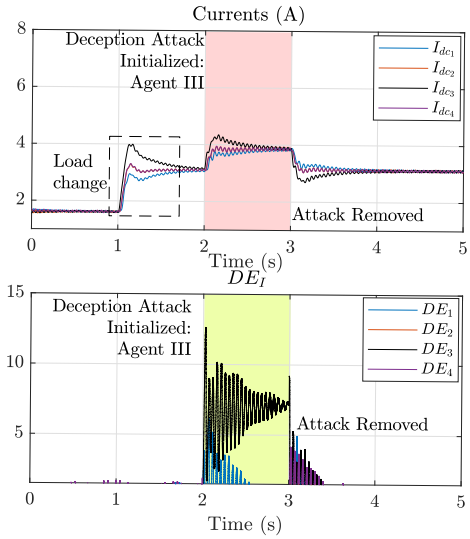

Fig. 11. Performance of the proposed detection strategy for a maximum communication delay of 120 ms under deception attack (***IA*** = 2) in agent III– Positive DE_I for agent III indicates the presence of attack.

attacks is tested when agent I is plugged in and out at t = 2 and 3.5 s respectively in Fig. 9. In realistic scenarios, these cases may arise when input sources such as batteries

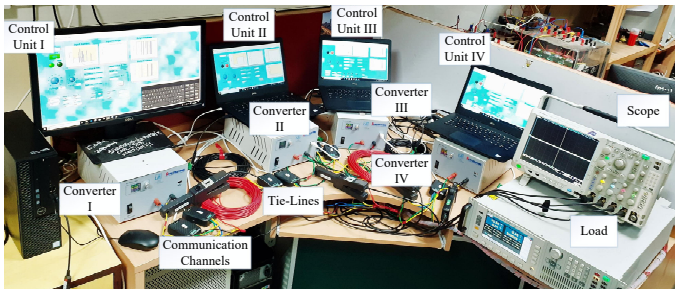

Fig. 12. Experimental setup comprising of four commercial DC/DC converters connected in parallel in a ring circuit. They are controlled via four separate control units to maintain output voltage using a ring-based distributed cyber network between them to supply power to the programmable DC load.

run out of charging capacity. This mandates plugging out of the respective agent from the system. In Fig. 9, it can be observed that DE_I^4 becomes positive as soon as the attack $I_{dc_4}^a$ = 1.2 A is initiated in agent IV. It is worth notifying that the communication links and control is lost for the plugged out agent. Under this condition, DE_I in (22) will only be calculated for the active agents. As a result, DE_I in (22) does not account for any measurements from agent I while it is plugged out. However, when agent I is restored back into the system with control and communication link enabled, it can be seen that the proposed discordant element is still positive only for the attacked agent. It is worth mentioning that a dwell time of 1 s is used for the proposed detection strategy to avoid chattering of signals and improve the accuracy of detection.

Following the preliminaries of well-defined detection strategies in large power systems [20], it is impossible to detect an attack if more than half the sensors/actuators are compromised. To test the effectiveness of the proposed detection strategy for the highest level of intrusion access index (***IA*** = 3), all the current sensors and cyber-links are attacked sequentially at t = {1, 1.5, 2, 2.5} s. Using the risk assessment framework in Scenario B, it can be concluded that such attacks have the potential to cause maximum risk without being identified (***RA*** = 9). It can be seen in Fig. 10 as soon as the attack is initiated in each agent, corresponding DE_I goes positive. However, the attack conducted at t = 2 and 2.5 s in a wholly attacked system creates a misconduct for the proposed detection strategy as only DE_I^1 and DE_I^3 go up in the positive region. As a matter of fact, the proposed strategy doesn't provide an unified picture

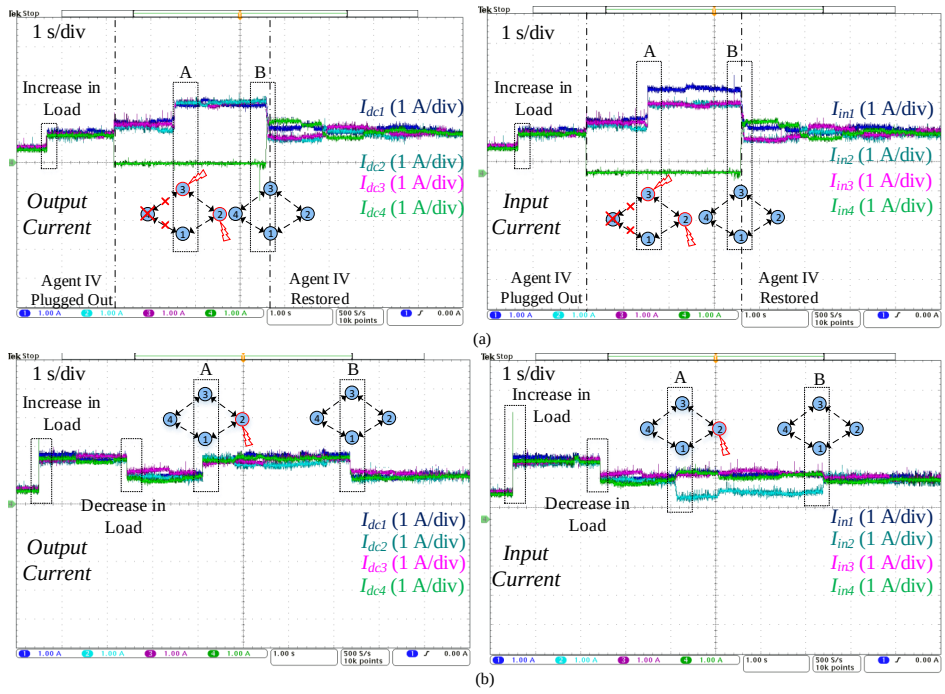

Fig. 13. Experimental validation of the proposed DE based detection theory with input and output currents: (a) Deception attack (***IA*** = 3) on agent II and III when agent IV is plugged in-and-out, and (b) Deception attack (***IA*** = 2) on agent II under a maximum communication delay of 65 ms. Positive DE_I for the attacked agents [calculated using (22)] ensures the presence of attack element in the corresponding agents from event A-B.

of the actual event. This depicts its limitation with its operation bounded to a certain number of compromised cyber-physical components, which is established when the attack is removed in Fig. 10. Operating as per the detection criteria during t = 2.5-3.5 s, since DE_I^1 and DE_I^3 are in the positive region, the attack in agent III is removed first. As soon as it is removed, DE_I for the rest of the agents go up into the positive region. Finally at t = 5 s, when all the attack elements are removed, the output currents are shared in magnitude similar to the pre-attack scenario.

Referring to Fig. 11, the reliability of the proposed strategy is examined when subjected to a maximum communication delay of 120 ms in the ring-based cyber network. Since delay affects the performance of the distributed controller, the system operation is always carried out within a borderline delay such that the convergence is guaranteed using consensus theory [18]. Within the said borderline delay range, the rate of convergence is directly proportional to the communication delay. To test this theory, a deception attack is carried out on agent III at t = 2 s in Fig. 11. It can be seen that even with a slower rate of convergence owing to the communication delay, a positive value for DE_I^3 confirms the presence of attack in agent III. Hence, it can be concluded that the performance of proposed detection scheme will remain unaffected by communication delay as long as the convergence is reached to obey the system objectives in (6).

VI. Experimental Results

The proposed detection strategy has also been experimentally validated in a DC microgrid with $N = 4$ agents, as shown in Fig. 12. To demonstrate the inconsiderable ease of implementation of these attacks and the proposed detection strategy, the experimental prototype is carried out with four commercial DC/DC boost converters [21] tied in parallel in a physical ring-bus network comprising a programmable load (voltage-dependent mode) in one of the buses. The reference voltage for each converter, given by (5), can be varied in their respective control units, as shown in Fig. 12. Each analog measurement from each converter is communicated to their neighboring control units using USB accompanying the *Modbus* protocol to execute undirected distributed communication. Using the local and neighboring measurements, the secondary sublayers shown in Fig. 3 is modeled in the LabVIEW platform to vary the voltage references for each agent to meet the control objectives in (6) accordingly. To implement destabilization attacks, the current measurements are manipulated locally in the respective control unit. On the other hand, the current signals are manipulated both for the local and communicated measurements in case of deception attacks. It is worth notifying that since the commercial DC/DC converters didn't have an acquisition channel, the experimental results have been shown in terms of measurable quantities, which provides a basic understanding of the proposed discordant theory. The value of DE_I can be calculated using (22) in the waveforms of input currents with $l = 1.2$. In the following results, event A depict the instant where the false data is injected to initiate the attack and event B depict the instant where the attack is removed. The experimental testbed parameters are provided in Appendix.

In Fig. 13(a), the performance of the proposed detection scheme is evaluated during a converter outage and restoration. As soon as agent IV is plugged out, the remaining active

agents share the load equally in terms of both input and output currents. However, when a deception attack of $I^a_{dc_2}$ = 0.25 A and $I^a_{dc_3}$ = 0.5 A is injected into agent II and III respectively, it can be seen that even though output currents are shared proportionately, the input currents of agents II and III are in *discord* with agent I. As already mentioned in Section V, the communication and control is lost for agent IV, which restricts the calculation of DE_I only for active agents. Further at event B, when the attack is removed and the agent IV is restored back at event B, the input and output currents return back to normal operation by sharing their currents equally. This demonstrates that the proposed detection scheme performs normally even under plug in-and-out of agents in DC microgrids.

In Fig. 13(b), all the current counterparts in agent II, including output current sensors and cyber link, are injected with a false data of I^a_{dc} = 0.5 A during event A. The system is operating with a maximum communication delay of 65 ms. Using Remark II, the control objectives of the system is still achieved as the output currents from each agent are shared proportionately. However as per the proposed detection theory, the input current of agent II goes in *discord* with the input currents of remaining agents, which renders a positive value for DE^2_I as per (22) between events A to B. Hence, it can be concluded that the attack detection philosophy performs normally under experimental conditions even in the presence of communication delay.

VII. Conclusions and Future Scope of Work

This paper presents a discordant element based detection theory to detect two categories of false data injection attacks, namely *destabilization* and *deception* attacks in cyber-physical DC microgrids. Since such attacks can impose risk on critical infrastructure, a risk assessment framework is provided to quantify the impact of each attack in autonomous microgrids. Furthermore, a theoretical analysis is carried out for cooperative microgrids to analyze the system response based on the symmetric nature of attack vector into the current sensors and cyber links. The necessary conditions to model both variants of attack is studied in detail. Using these discussions, a unified and fully distributed discordant element based detection theory is devised to detect the possibility of false data in the network using extended analysis of consensus theory for the controller equations. A detailed study is done to differentiate the cyber attacks from line-to-line faults to avoid false tripping of relays. Since it operates only using local and neighboring measurements, this detection strategy can be scaled up to any number of agents in DC microgrids. It has been simulated for various test cases of attacks to explain its critical boundaries of detection under different intrusion access indices. Moreover, the proposed philosophy is carried out in commercial DC/DC converters to demonstrate the ease of implementation of the detection philosophy with minimal effort. This technique can potentially be a great asset for naval DC microgrids with security as primary concern. To extend future scope of this work, theoretical evaluation and validation of sensor failures and differentiation with cyber attacks will be carried out.

Appendix

Simulation Parameters

The considered system consists of four sources rated equally for 5 kW. It is to be noted that the line parameter R_{ij} is connected from i^{th} agent to j^{th} agent. Moreover, the controller gains are consistent for each agent.

Plant: R_{12} = 1.8 Ω, R_{14} = 1.3 Ω, R_{23} = 2.3 Ω, R_{43} = 2.1 Ω
Converter: L_{se_i}= 3 mH, C_{dc_i}= 250 μF, i^{max}_{dc} = 16 A
Controller: $V_{dc_{ref}}$= 315 V, $I_{dc_{ref}}$ = 0, $K^{H_1}_P$ = 3, $K^{H_1}_I$ = 0.01, $K^{H_2}_P$ = 4.5, $K^{H_2}_I$ = 0.32, G_{VP} = 2.8, G_{VI} = 12.8, G_{CP} = 0.56, G_{CI} = 21.8, V_{in} = 270 V, g = 2.4, l = 3.24.

Experimental Testbed Parameters

The considered system consists of four sources with the converters rated equally for 1 kW. It should be noted that the controller gains are consistent for each agent.

Plant: L_{se_i}= 3 mH, C_{dc_i}= 100 μF
Controller: $V_{dc_{ref}}$= 48 V, $I_{dc_{ref}}$ = 0, $K^{H_1}_P$ = 240.6, $K^{H_1}_I$ = 1.6, $K^{H_2}_P$ = 4.5, $K^{H_2}_I$ = 0.08, g = 2, l = 1.2, V_{in} = 36 V.

References

[1] T Dragicevic, X Lu, JC Vasquez, JM Guerrero, "DC microgrids–Part I: A review of control strategies and stabilization techniques", *IEEE Trans. on Power Elect.*, vol. 31, no. 7, pp. 4876-4891, 2016.

[2] M. Yazdanian and A. Mehrizi-Sani, "Distributed Control Techniques in Microgrids," *IEEE Trans. on Smart Grid*, vol. 5, no. 6, pp. 2901–2909, 2014.

[3] S Sahoo and S. Mishra, "A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids", *IEEE Trans. on Smart Grid*, 2017. DOI: 10.1109/TSG.2017.2737938

[4] V. Nasirian, S. Moayedi, A Davoudi and F. L. Lewis, "Distributed Cooperative Control of DC Microgrids," *IEEE Trans. on Power Elect.*, vol. 30, no. 4, pp. 2288–2303, 2015.

[5] S Anand, BG Fernandes, and JM Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids." *IEEE Trans. on Power Elect.*, vol. 28, no. 4, pp. 1900-1913, 2013

[6] X Zhong, et al, "Cyber security in smart DC microgrid operations", *DC Microgrids (ICDCM), 2015 IEEE First Intl. Conf. on*, 2015.

[7] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," *Sandia Nat. Lab.(Hierarch. SNLNM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472*, 2013.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Inf. Syst. Security*, vol. 14, no. 1, p. 13, 2011.

[9] P Danzi, M Angjelichinoski, C Stefanovic, T Dragicevic, and P Popovski, "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks" *IEEE Trans. Smart Grid*, 2018.

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. on Autom. Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[11] MM Rana, L Li, and SW Su, "Cyber attack protection and control of microgrids", *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 2, pp. 602-609, 2018.

[12] Sun, Ke, et al. "Stealth Attacks on the Smart Grid." *arXiv preprint arXiv:1808.04184*, 2018.

[13] S Sahoo, S Mishra, JCH Peng, and T Dragicevic, "A Stealth Attack Detection Strategy for DC Microgrids", *IEEE Trans. Power Electron.*, vo. 34, no. 8, pp. 8162-8174, Aug 2019.

[14] O. Beg, T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. on Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, 2017.

[15] O Beg, et al. "Signal Temporal Logic-based Attack Detection in DC Microgrids", *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585-3595, July 2019.

[16] B Satchinandan, and Panganamala R. Kumar. "Dynamic watermarking: Active defense of networked cyber-physical systems." *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219-240, 2017.

[17] NL Diaz, et al, "Intelligent distributed generation and storage units for DC microgrids–A new concept on cooperative control without communications beyond droop control," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2476-2485, 2014.
[18] S Sahoo, S Mishra, S Jha, B Singh, "A Cooperative Adaptive Droop Based Energy Management & Optimal Voltage Regulation Scheme for DC Microgrids", *IEEE Trans. on Ind. Electr.*, pp. 1-1, 2019.
[19] M Zhu, and S Martinez, "Discrete-time dynamic average consensus", *Automatica*, vol. 46, no. 2, pp. 322-329, 2010.
[20] B Zhu, A Joseph and S Sastry, "A taxonomy of cyber attacks on SCADA systems", *Internet of Things, 2011 Intl. Conf.*, 2011.
[21] Silov Solutions Pvt. Ltd., 2018. [Online] Available: http://www.silovsolutions.com/

Subham Sahoo (S'16-M'18) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSS University of Technology, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018 respectively. He has worked as a visiting student with the Department of Electrical and Electronics Engineering in Cardiff University, UK in 2017 and as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore in 2018-2019. He is currently working as a research fellow in the Department of Energy Technology, Aalborg University, Denmark.

His current research interests include microgrids, cyber security, control and stability of cyber-physical systems.

Jimmy Chih-Hsien Peng (M'04) is currently an Assistant Professor of Electrical and Computer Engineering at the National University of Singapore, Singapore. Previously, he was a faculty at the Masdar Institute (now part of the Khalifa University), United Arab Emirates. In 2013, he was appointed as a Visiting Scientist with the Research Laboratory of Electronics at the Massachusetts Institute of Technology (MIT), Massachusetts. He later became a Visiting Assistant Professor at MIT in 2014.

He currently serves as the secretary for IEEE Power and Energy Society Working Group on High-Performance Computing for Power Grid Analysis and Operation. He is also a committee member for Singapore Standard SS 535. His research interests include power system stability, cyber security, microgrids, and high-performance computing.

Annavaram Devakumar received the M.Tech. degree in Electrical Power System from the Jawaharlal Nehru Technological University, Anantapur, India, in 2017. He is currently working toward the Ph.D. degree at Indian Institute of Technology Delhi, New Delhi, India.

His research interests include application of power electronics in power systems and control of cyber-physical AC/DC microgrids.

Sukumar Mishra (M'97-SM'04) is a Professor at Indian Institute of Technology, New Delhi and has been part of IIT Delhi for the past 15 years. He has published over 200 research articles (including papers in international journals, conferences and book chapters).

Prof. Mishra has won many accolades throughout his academic tenure of 25 years. He has been a recipient of INSA medal for young scientist (2002), INAE young engineer award (2009), INAE silver jubilee young engineer award (2012) and has recently won the Samanta Chandra Shekhar Award (2016). He has been granted fellowship from many prestigious technical societies like IET (UK), NASI (India), INAE (India), IETE (India) and IE (India) and is also recognized as the INAE Industry Academic Distinguish Professor. Apart from all research and academic collaborations, Prof. Mishra is very actively involved in industrial collaborations. Prof. Mishra is currently acting as NTPC Chair professor and has previously delegated as the Power Grid Chair professor. He is also serving as an Independent Director of the Cross Border Power Transmission Company Ltd. and the River Engineering Pvt. Ltd. Prof. Mishra has also carried out many important industrial consultations with TATA Power, Microtek and others. Prof. Mishra?s research expertise lies in the field of Power Systems, Power Quality Studies, Renewable Energy and Smart Grid. He is currently serving as an Editor for the IEEE Transactions on Smart Grid, IEEE Transactions on Sustainable Energy and an Associate Editor for the IET Generation, Transmission & Distribution journal.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral research associate at Aalborg University, Denmark. From March 2016, he is an Associate Professor at Aalborg University, Denmark where he leads an Advanced Control Lab.

He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His principal field of interest is design and control of microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and co-authored more than 170 technical papers (more than 70 of them are published in international journals, mostly IEEE Transactions) in his domain of interest, 8 book chapters and a book in the field.

He serves as an Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Dr. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, and a Robert Mayer Energy Conservation award.